Advt. No. N-22030/149/2024-DIC
Digital India Corporation
Electronics Niketan Annexe, 6, CGO Complex Lodhi Road, New
Delhi – 110003 (Registered Office)
Tel.: +91 120 654 0800
Website: www.dic.gov.in

Web Advertisement
03.11.2026

Digital India Corporation has been set up by the 'Ministry of Electronics & Information Technology, Government of India', to innovate, develop and deploy ICT and other emerging technologies for the benefit of the common man. It is a 'not for profit' Company under Section 8 of the Companies Act 2013. The Company has been spearheading the Digital India programme of the Government of India, and is involved in promoting use of technology for e-Governance/e-Health / Telemedicine, e- agriculture, e-Payments etc. The Digital India programme promotes safety and security concerns of growing cashless economy and addresses challenges confronting its wider acceptance. It also promotes innovation and evolves models for empowerment of citizens through Digital initiatives and promotes participatory governance and citizen engagement across the government through various platforms including social media.

Digital India Corporation is currently inviting applications for the following positions purely on Contract/ Consolidated basis:-

Sr. No.	Name of the Post	Number of Position
1	Product Manager	01
2	Full Stack Developer	01
3	QA Tester	01
4	Application Security (AppSec) Specialist	01
5	DevSecOps Engineer	01
6	Platform & Security Engineer	01
7	Manager — Development, Support & Onboarding	01
8	Junior: Backend / Mobile Developer	01
9	Junior: QA & Security Support	01
10	Junior: L1 / L2 Application Support	01
11	Frontend Developer	01

** The place of posting shall be in Delhi/NCR but transferable to project locations of Digital India Corporation as per existing policy of Digital India Corporation.

Shortlisting shall be carried out through an objective evaluation matrix based on educational qualification, relevant experience, domain expertise, certifications, publications, and other criteria as approved by the Competent Authority. Mere fulfillment of eligibility conditions shall not confer any right to be shortlisted.

Digital India Corporation reserves the right to fix higher threshold of qualifications and experience for screening and limiting the number of candidates for interview. DIC reserves the right not to fill the post without assigning any reason thereof. The decision of DIC regarding shortlisting shall be final and binding. Only shortlisted candidates shall be invited for selection interviews.

The details can be downloaded from the official website of DIC, NeGD, MyGov & MeitY viz. www.dic.gov.in, www.negd.gov.in, www.mygov.in, & www.meity.gov.in

Eligible candidates may apply ONLINE: **https://ora.digitalindiacorporation.in/**

Last date of Receipt of Applications: 18. 11. 2026

1. Job Title:	Product Manager
No. of Posts:	1

Job Description

About the Platform

The Digital Office Platform is a multi-tenant, configuration-driven government case-management platform that lets many independent government bodies each configure their own case lifecycle — data model, intake forms, versioned workflows, roles, SLAs, notifications, audit and reporting — and run real cases end-to-end without custom code per tenant. It is built as ~20 independent Spring Boot microservices (engines), each owning its own PostgreSQL database, coordinated behind a Next.js web application, and deployed hosting-agnostic on sovereign / government cloud using open-source components. Tenant isolation is by tenant_id; published workflow versions are immutable and live cases pin to their version; security and data boundaries fail closed.

Role and Responsibilities

1. Elicit, analyse and document requirements for each onboarding government body; prepare the BRD / FRD with unique requirement IDs, acceptance criteria and a requirement traceability matrix linking every requirement to a design element and a test case.
2. Translate each body's case lifecycle into configuration — business object types and fields, dynamic intake forms (sections, rows, columns, conditional visibility, calculated fields), versioned workflows (stages, tasks, actions, transitions), roles / personas, rules / decision tables, SLAs, notification templates and dashboards — so a new office is stood up by configuration, not code.
3. Define the workflow-versioning and in-flight case-migration policy: published versions are immutable, live cases pin to the version in force when filed, and any migration between versions is explicit, mapped stage-to-stage and audited.
4. Specify SLA, clarification, escalation and reminder rules, and the notification matrix (EMAIL / SMS / WhatsApp / push / in-app / webhook) per workflow stage and actor class.
5. Specify role-based access needs across the four actor classes — platform admin, tenant staff, citizens / applicants, and second parties / respondents — and the RBAC / ABAC / policy model with the IAM owner.
6. Define reporting and dashboard requirements as curated, tenant-scoped datasets and named metrics (never ad-hoc cross-tenant SQL), and the KPIs each role needs.
7. Own the product roadmap, MoSCoW prioritisation, release phasing and scope discipline across the ~20 engines; chair backlog grooming and sprint planning.
8. Coordinate stakeholders across government bodies, DIC and the platform team; plan and drive UAT, capture sign-off, and manage change requests through a controlled process.
9. Author and maintain product documentation — user manuals per actor class, configuration playbooks, release notes and onboarding guides.

Qualifications and Experiences

1. Bachelor's degree in any discipline with 5+ years of experience in business analysis / product management for enterprise or government IT systems; experience with case-management, grievance-redressal or workflow platforms preferred.

Required Skill Set

1. Strong requirements engineering and documentation (requirement specifications, manuals, traceability) and stakeholder management across technical and non-technical audiences.
2. Business-process and workflow modelling (BPMN an advantage); ability to express case lifecycles as configuration rather than code.
3. Working understanding of multi-tenant SaaS, metadata / configuration-driven platforms, RBAC / ABAC, SLA design and notification workflows.
4. Knowledge of GIGW, accessibility and DPDP (Act 2023 / Rules 2025) compliance as they affect requirements.
5. Comfortable reading REST API contracts, data models and configuration schemas; proficient with Agile tooling (Jira / Confluence).

Consolidated Remuneration:

1. Consolidated remuneration shall be commensurate with qualifications and experience within the approved project norms.

2. Job Title:	**Full Stack Developer**
No. of Posts:	1
Job Description	

About the Platform

The Digital Office Platform is a multi-tenant, configuration-driven government case-management platform that lets many independent government bodies each configure their own case lifecycle — data model, intake forms, versioned workflows, roles, SLAs, notifications, audit and reporting — and run real cases end-to-end without custom code per tenant. It is built as ~20 independent Spring Boot microservices (engines), each owning its own PostgreSQL database, coordinated behind a Next.js web application, and deployed hosting-agnostic on sovereign / government cloud using open-source components. Tenant isolation is by tenant_id; published workflow versions are immutable and live cases pin to their version; security and data boundaries fail closed.

Role and Responsibilities

1. Develop and enhance backend engines in Java 21 and Spring Boot 3.3 (Spring Data JPA / Hibernate, Spring Security + JWT), following the shared clean-architecture layering (api → application → domain → infrastructure), the standard { success, data } response envelope and the domain-exception pattern used across the fleet.
2. Build and extend core engine capabilities — business objects (dynamic object types, fields and JSONB records with versioning and audit), dynamic forms, versioned workflows and tasks, rules / decision tables, documents, notifications, search, reporting, dashboards, scheduler and integrations — as configuration-driven features.
3. Develop web services and REST APIs with auto-generated OpenAPI (SpringDoc) docs, and build typed, fail-closed inter-engine clients; respect database-per-engine ownership (no cross-engine database reads — consume curated, tenant-scoped HTTP datasets).
4. Develop the web application in Next.js 16 / React 19 with TypeScript, Tailwind CSS, Zustand, react-hook-form + zod and recharts — dynamic tenant-configured forms, workflow and case screens, dashboards and the per-engine service / API-client layer, serving all four actor classes.
5. Implement and uphold tenant-scoped persistence: every query carries a bound tenant predicate, identifiers are allow-listed and never string-interpolated, and sensitive provider secrets are handled via the platform's encrypted, fail-closed mechanisms.
6. Author Flyway migrations for the production path and keep the entity model, repositories and schema consistent; use UUID identifiers and per-engine schemas per the established conventions.
7. Integrate third-party and government services (SMS / email / SSO / payment / external APIs) through the integration engine with retry, circuit-breaker and data-transformation patterns; wire Redis caching and Apache Kafka event flows for cross-engine reactions (notifications, indexing, audit).
8. Apply AI-assisted code review and technical enhancements; write unit and integration tests, participate in code reviews, and uphold secure-by-design and fail-closed coding practices.
9. Work across the complete SDLC — functional and technical specifications, documentation, QA support, source control, maintenance and deployments.

9. Work across the complete SDLC — functional and technical specifications, documentation, QA support, source control, maintenance and deployments.

Qualifications and Experiences

1. Bachelor's degree in any discipline with 3+ years of experience in full-stack web application development using Java / Spring Boot and React / Next.js.

Required Skill Set

1. Strong proficiency in Java 21, Spring Boot 3.3, Hibernate / JPA, Spring Security + JWT, and REST web-service development with OpenAPI.
2. Proficiency in Next.js / React, TypeScript, HTML, CSS, JavaScript, Tailwind, Zustand and react-hook-form + zod.
3. Solid working experience with relational databases (PostgreSQL 16), JSONB and GIN indexing, and version-control tools (Git).
4. Understanding of microservice architecture and integration, multi-tenant isolation, clean / layered architecture, and configuration / metadata-driven design.
5. Familiarity with Redis, Apache Kafka, Docker, and performance (JMeter / Gatling), functional, unit and integration testing.
6. Awareness of W3C / GIGW and accessibility guidelines and of Agile delivery.

Desirable Skill Set

- Experience with workflow / BPM and rules engines (Camunda, Flowable, Drools).
- Experience building dynamic form / metadata-driven systems and document / search / notification subsystems.
- Experience using AI-assisted development and code-review tools.

Consolidated Remuneration:

1. Consolidated remuneration shall be commensurate with qualifications and experience within the approved project norms.

3. Job Title:	QA Tester
No. of Posts:	1

Job Description

About the Platform

The Digital Office Platform is a multi-tenant, configuration-driven government case-management platform that lets many independent government bodies each configure their own case lifecycle — data model, intake forms, versioned workflows, roles, SLAs, notifications, audit and reporting — and run real cases end-to-end without custom code per tenant. It is built as ~20 independent Spring Boot microservices (engines), each owning its own PostgreSQL database, coordinated behind a Next.js web application, and deployed hosting-agnostic on sovereign / government cloud using open-source components. Tenant isolation is by tenant_id; published workflow versions are immutable and live cases pin to their version; security and data boundaries fail closed.

Role and Responsibilities

1. Prepare the test strategy and test plans; design and execute functional, regression and integration test cases across all engines and the web application, mapped to acceptance criteria and requirement IDs.
2. Design and execute the cross-tenant isolation test suite — a session for one tenant must never read, filter into, list or mutate another tenant's data across any engine or API; treat any leak as a build-blocking defect.
3. Test the dynamic configuration surface end-to-end: business object types and fields, dynamic forms (conditional visibility, calculated fields, validation), rules / decision tables, notification templates and dashboards — verifying that configuration, not code, drives behaviour.
4. Test versioned-workflow execution and in-flight case migration: version immutability, cases pinning to their filed version, stage / task / action / transition correctness, SLA timers, clarification and escalation paths, and the always-valid START → END spine.
5. Test authentication and authorization across the four actor classes and the RBAC / ABAC matrix; verify fail-closed behaviour (deny by default, honest "unavailable" responses).
6. Test documents (upload, checksum, versioning), notifications (multi-channel dispatch and templates), search (relevance, highlighting, autocomplete), reporting and dashboards for correctness and tenant scoping.
7. Own release testing and regression cycles across the ~20 engines; build automation with suitable API / UI frameworks and in-memory (H2) or containerised databases; support performance testing.
8. Log, track and verify defects to closure using defect-tracking tools; maintain traceability from requirement to test to defect; support UAT and release sign-off.

Qualifications and Experiences

1. Bachelor's degree in any discipline with 3+ years of experience in software quality assurance / testing of web and API-based systems.

Required Skill Set

1. Strong test design and execution across functional, regression, integration and release testing.
2. REST API testing (Postman / REST-assured), test automation frameworks and E2E tools (Playwright or equivalent).
3. Understanding of multi-tenant isolation testing, workflow / BPM testing and RBAC / authorization testing.

4. Familiarity with PostgreSQL, bug-reporting / test-management tools, and CI-integrated test execution; awareness of performance-testing tools (JMeter/ Gatling).

Consolidated Remuneration:

1. Consolidated remuneration shall be commensurate with qualifications and experience within the approved project norms.

4. Job Title:	Application Security (AppSec) Specialist
No. of Posts:	1

Job Description

About the Platform

The Digital Office Platform is a multi-tenant, configuration-driven government case-management platform that lets many independent government bodies each configure their own case lifecycle — data model, intake forms, versioned workflows, roles, SLAs, notifications, audit and reporting — and run real cases end-to-end without custom code per tenant. It is built as ~20 independent Spring Boot microservices (engines), each owning its own PostgreSQL database, coordinated behind a Next.js web application, and deployed hosting-agnostic on sovereign / government cloud using open-source components. Tenant isolation is by tenant_id; published workflow versions are immutable and live cases pin to their version; security and data boundaries fail closed.

Role and Responsibilities

1. Threat-model the platform end-to-end and review the secure design of multi-tenancy (tenant_id isolation and bound tenant predicates), the deny-by-default / fail-closed security filters, and the separated three- key trust model (fleet JWT secret, platform-admin signing key, internal-service key — kept distinct and never merged).
2. Conduct secure code reviews across the Java / Spring engines and the Next.js application — covering authentication (BCrypt password hashing, lockout, session limits, token lifecycle), authorization (RBAC / ABAC / policy), input validation, injection prevention (allow-listed identifiers, parameterised queries) and secret handling (AES-256-GCM at rest) — and drive remediation to closure.
3. Plan and coordinate VAPT / penetration testing and vulnerability assessments across the fleet and the web / API surface; triage SAST / DAST / SCA findings, assign severities and track fixes.
4. Own DPDP (Act 2023 / Rules 2025) compliance review — data-flow and data-inventory mapping, consent, retention, data-minimisation and cross-tenant data-isolation controls — and the immutable audit trail (append-only store, SHA-256 integrity, field-level diff).
5. Review and advise on the documented residual hardening items (e.g. RS256 / JWKS token hardening and token revocation, platform MFA) and verify closure as they are addressed; define the secure-coding and security-testing standards the team follows.
6. Prepare security evidence and documentation for STQC clearance and government security audit, and support incident response for security events.

Qualifications and Experiences

1. Bachelor's degree in any discipline with 5+ years of experience in application security / secure software development.

Required Skill Set

1. Strong knowledge of OWASP Top 10, secure coding in Java / Spring, JWT / token security, and session / credential security.
2. Experience in multi-tenant data-isolation review and in handling web / API security audits and their tools.
3. Experience planning and coordinating VAPT / penetration testing and using SAST / DAST / SCA tooling.
4. Working knowledge of DPDP Act 2023 / Rules 2025, GIGW and STQC requirements, and of cryptographic controls (hashing, authenticated encryption, key management).

Consolidated Remuneration:

1. Consolidated remuneration shall be commensurate with qualifications and experience within the approved project norms.

5. Job Title:	DevSecOps Engineer
No. of Posts:	1

Job Description

About the Platform

The Digital Office Platform is a multi-tenant, configuration-driven government case-management platform that lets many independent government bodies each configure their own case lifecycle — data model, intake forms, versioned workflows, roles, SLAs, notifications, audit and reporting — and run real cases end-to-end without custom code per tenant. It is built as ~20 independent Spring Boot microservices (engines), each owning its own PostgreSQL database, coordinated behind a Next.js web application, and deployed hosting-agnostic on sovereign / government cloud using open-source components. Tenant isolation is by tenant_id; published workflow versions are immutable and live cases pin to their version; security and data boundaries fail closed.

Role and Responsibilities

1. Design, build and maintain CI/CD pipelines that compile (Maven), test, security-scan (SAST / DAST / dependency scanning) and containerise each of the ~20 engines as a reproducible, multi-stage Docker image, with uniform pipeline shape across the fleet.
2. Automate deployment across environments using Docker / Docker Compose (local and CI) and Kubernetes (production) — declarative manifests, health-managed rollout, auto-scaling, self-healing and zero / low-downtime release strategies.
3. Own release management across the fleet — semantic versioning, environment promotion (dev → staging → production), controlled rollback, and mirroring dev schema changes into Flyway for the production path.
4. Manage secrets and the separated three-key trust model within the pipeline, and the AES-256-GCM secret-encryption key configuration; enforce that engines fail closed when required keys or secrets are absent.
5. Automate environment provisioning (Infrastructure-as-Code) and consistently wire the data and messaging estate — PostgreSQL per engine, Redis and Apache Kafka / Zookeeper — across environments.
6. Build pipeline and runtime observability (logs, metrics, traces, alerts) and embed security and quality gates so a critical finding blocks promotion.
7. Partner with the Platform & Security Engineer on production topology and with AppSec on pipeline security controls and evidence for audit.

Qualifications and Experiences

1. Bachelor's degree in any discipline with 4+ years of experience in DevOps / DevSecOps for microservice-based systems.

Required Skill Set

1. Strong hands-on Docker and Kubernetes; CI/CD pipelines (GitLab CI / Jenkins / GitHub Actions) with integrated security scanning, on self-hosted runners and registries.
2. Secrets management, Infrastructure-as-Code (Terraform / Ansible), and release-management discipline (Flyway-based change control, promotion, rollback).
3. Experience operating Apache Kafka and Redis and deploying Spring Boot + Next.js workloads on sovereign / government cloud.
4. Observability stacks (Prometheus / Grafana / ELK) and build-time security tooling.

Consolidated Remuneration:

1. Consolidated remuneration shall be commensurate with qualifications and experience within the approved project norm

6. Job Title:	Platform & Security Engineer
No. of Posts:	1

Job Description

About the Platform

The Digital Office Platform is a multi-tenant, configuration-driven government case-management platform that lets many independent government bodies each configure their own case lifecycle — data model, intake forms, versioned workflows, roles, SLAs, notifications, audit and reporting — and run real cases end-to-end without custom code per tenant. It is built as ~20 independent Spring Boot microservices (engines), each owning its own PostgreSQL database, coordinated behind a Next.js web application, and deployed hosting-agnostic on sovereign / government cloud using open-source components. Tenant isolation is by tenant_id; published workflow versions are immutable and live cases pin to their version; security and data boundaries fail closed.

Role and Responsibilities

1. Design and operate the hosting-agnostic environment on private / sovereign / government cloud: compute, network topology and segmentation, firewalls, TLS / ingress, DNS and strict environment separation (dev / staging / production).
2. Operate the self-managed data and messaging estate at fleet scale — PostgreSQL 16 with HA / streaming replication (one database per engine), Redis (Sentinel / Cluster) and a multi-broker Apache Kafka cluster — with capacity planning, tuning and growth headroom for ~20 services.
3. Own platform availability (target uptime, health management, self-healing), monitoring, alerting and capacity management across the fleet; ensure the append-only audit store and its immutability triggers are protected and backed up.
4. Own backup and disaster-recovery architecture and rehearsed restore drills; define and prove RPO / RTO targets and maintain the DR runbook.
5. Own platform-layer and infrastructure security — hardening, network policy, least-privilege access, and the custody, storage and rotation of the platform-admin signing key, internal-service key and encryption keys (separated from the runtime application).
6. Define and enforce the production topology and scaling model (replicas for IAM / workflow / business-object and other high-load engines) and partner with DevSecOps on deployment and with AppSec on end-to-end hardening and audit evidence.

Qualifications and Experiences

1. Bachelor's degree in any discipline with 6+ years of experience in infrastructure / platform engineering with a strong security focus; experience operating production microservice fleets preferred.

Required Skill Set

1. Hosting-agnostic experience on private / sovereign / government cloud (VMware, OpenStack or KVM) and Kubernetes — without dependence on public-hyperscaler managed services.
2. Deep self-managed PostgreSQL (HA, streaming replication, many databases); Redis and Apache Kafka operations; strong Linux and networking.
3. Infrastructure-as-Code (Terraform / Ansible), backup / DR tooling, and self-hosted observability (Prometheus / Grafana / ELK).
4. Key-management and secrets custody; familiarity with STQC / DPDP infrastructure controls and data-residency requirements.

7. Job Title:	Manager — Development, Support & Onboarding
No. of Posts:	1

Job Description

About the Platform

The Digital Office Platform is a multi-tenant, configuration-driven government case-management platform that lets many independent government bodies each configure their own case lifecycle — data model, intake forms, versioned workflows, roles, SLAs, notifications, audit and reporting — and run real cases end-to-end without custom code per tenant. It is built as ~20 independent Spring Boot microservices (engines), each owning its own PostgreSQL database, coordinated behind a Next.js web application, and deployed hosting-agnostic on sovereign/government cloud using open-source components. Tenant isolation is by tenant_id; published workflow versions are immutable and live cases pin to their version; security and data boundaries fail closed.

Role and Responsibilities

1. Provide technical coordination across development, tenant onboarding / provisioning (the admin-portal onboarding and provisioning flow) and L1 / L2 / L3 support, running them as one integrated service for the platform.
2. Own tenant onboarding and the provisioning lifecycle — from request through configuration (object types, forms, workflows, roles, branding) to go-live — with segregation of duties preserved, so platform-admin provisioning privilege is held and operated separately from development.
3. Own incident management and escalation, problem management and the change-advisory process; monitor and report SLAs across tenants and engines.
4. Coordinate release-to-support handover, maintain runbooks and the knowledge base, and drive continuous service improvement across the ~20 engines.
5. Plan capacity and rosters for the support tiers (including the three junior resources), run the government reporting cadence, and act as the primary coordination point between government bodies, DIC and the engineering team.
6. Track service metrics (uptime, ticket volumes, resolution times, SLA adherence) and drive remediation of recurring issues.

Qualifications and Experiences

1. Bachelor's degree in any discipline with 8+ years of experience in IT delivery / service-delivery management.

Required Skill Set

1. Strong ITIL / service delivery, incident, problem, change and SLA management, and SDLC coordination.
2. Understanding of microservice platforms and multi-tenant onboarding sufficient to coordinate development, support and provisioning.
3. Strong stakeholder communication, reporting and team management across L1 / L2 / L3 support.
4. Experience managing onboarding / provisioning for multi-tenant or SaaS systems preferred.

Consolidated Remuneration:

1. Consolidated remuneration shall be commensurate with qualifications and experience within the approved project norm

8. Job Title:	Junior: Backend / Mobile Developer
No. of Posts:	1

Job Description

About the Platform

The Digital Office Platform is a multi-tenant, configuration-driven government case-management platform that lets many independent government bodies each configure their own case lifecycle — data model, intake forms, versioned workflows, roles, SLAs, notifications, audit and reporting — and run real cases end-to-end without custom code per tenant. It is built as ~20 independent Spring Boot microservices (engines), each owning its own PostgreSQL database, coordinated behind a Next.js web application, and deployed hosting-agnostic on sovereign / government cloud using open-source components. Tenant isolation is by tenant_id; published workflow versions are immutable and live cases pin to their version; security and data boundaries fail closed. This is one of three junior resources deployed against the L1 / L2 Support posts.

Role and Responsibilities

1. Make minor backend / API changes in Java / Spring Boot across engines, under the supervision of the Full Stack Developer, following the platform's clean-architecture and fail-closed conventions.
2. Provide mobile application support — issue triage, reproduction and resolution of reported defects.
3. Perform API testing and assist with diagnosis, bug-fixing and technical support.
4. Escalate true defects (L3) to the development team with clear reproduction detail, and verify fixes.

Qualifications and Experiences

1. Bachelor's degree in any discipline with 1–2 years of experience in backend / mobile development.

Required Skill Set

1. Exposure to Java / Spring Boot and REST APIs.
2. Basic understanding of PostgreSQL, Docker and mobile application support.
3. API testing tools (Postman) and sound troubleshooting aptitude.

Consolidated Remuneration:

1. Consolidated remuneration shall be commensurate with qualifications and experience within the approved project norm

9. Job Title:	Junior: QA & Security Support
No. of Posts:	1

Job Description

About the Platform

The Digital Office Platform is a multi-tenant, configuration-driven government case-management platform that lets many independent government bodies each configure their own case lifecycle — data model, intake forms, versioned workflows, roles, SLAs, notifications, audit and reporting — and run real cases end-to-end without custom code per tenant. It is built as ~20 independent Spring Boot microservices (engines), each owning its own PostgreSQL database, coordinated behind a Next.js web application, and deployed hosting-agnostic on sovereign / government cloud using open-source components. Tenant isolation is by tenant_id; published workflow versions are immutable and live cases pin to their version; security and data boundaries fail closed. This is one of three junior resources deployed against the L1 / L2 Support posts.

Role and Responsibilities

1. Execute test cases and run regression cycles across engines and the web application.
2. Verify defect fixes and support functional and release testing.
3. Perform basic security testing and assist the AppSec Specialist with VAPT remediation tracking and re-testing.
4. Assist with the cross-tenant isolation test runs, record findings and maintain test evidence.

Qualifications and Experiences

1. Bachelor's degree in any discipline with 1–2 years of experience in QA / testing.

Required Skill Set

1. Exposure to API and web testing and to defect-tracking / test-management tools.
2. Awareness of OWASP basics and security-testing concepts.
3. PostgreSQL basics and strong attention to detail.

Consolidated Remuneration:

1. Consolidated remuneration shall be commensurate with qualifications and experience within the approved project norm

10. Job Title:	Junior: L1 / L2 Application Support
No. of Posts:	1

Job Description

About the Platform

The Digital Office Platform is a multi-tenant, configuration-driven government case-management platform that lets many independent government bodies each configure their own case lifecycle — data model, intake forms, versioned workflows, roles, SLAs, notifications, audit and reporting — and run real cases end-to-end without custom code per tenant. It is built as ~20 independent Spring Boot microservices (engines), each owning its own PostgreSQL database, coordinated behind a Next.js web application, and deployed hosting-agnostic on sovereign / government cloud using open-source components. Tenant isolation is by tenant_id; published workflow versions are immutable and live cases pin to their version; security and data boundaries fail closed. This is one of three junior resources deployed against the L1 / L2 Support posts.

Role and Responsibilities

1. Provide front-line user support and handle tickets / incidents at L1 / L2, routing true defects to L3.
2. Monitor application health across engines, perform first-level troubleshooting and raise alerts.
3. Support tenant onboarding activities and user enablement across the actor classes.
4. Maintain the knowledge base, FAQs and support documentation, and track ticket resolution against SLAs.

Qualifications and Experiences

1. Bachelor's degree in any discipline with 1–2 years of experience in application / technical support.

Required Skill Set

1. Basic understanding of web applications, REST APIs and monitoring tools.
2. Strong communication and ticket-handling discipline; ITIL awareness an advantage.
3. Willingness to work in support rotations.

Consolidated Remuneration:

1. Consolidated remuneration shall be commensurate with qualifications and experience within the approved project norm

11. Job Title:	Frontend Developer
No. of Posts:	1

Job Description

About the Platform

The Digital Office Platform is a multi-tenant, configuration-driven government case-management platform that lets many independent government bodies each configure their own case lifecycle — data model, intake forms, versioned workflows, roles, SLAs, notifications, audit and reporting — and run real cases end-to-end without custom code per tenant. It is built as ~20 independent Spring Boot microservices (engines), each owning its own PostgreSQL database, coordinated behind a Next.js web application, and deployed hosting-agnostic on sovereign / government cloud using open-source components. Tenant isolation is by tenant_id; published workflow versions are immutable and live cases pin to their version; security and data boundaries fail closed.

Role and Responsibilities

1. Develop and maintain the platform's web application in Next.js 16 / React 19 with TypeScript, Tailwind CSS, Zustand and react-hook-form + zod, delivering responsive, accessible interfaces for all four actor classes (platform admin, tenant staff, citizens / applicants and second parties / respondents).
2. Build the dynamic, configuration-driven UI — render tenant-configured object types and forms (sections, rows, columns, conditional visibility, calculated fields, validation) from metadata, so new forms and fields appear without front-end code changes.
3. Implement workflow and case screens — stage / task / action views, transitions, SLA and status indicators, clarification and escalation flows — driven by the versioned-workflow configuration.
4. Build dashboards and reports in the UI using charting libraries (e.g. recharts), consuming curated, tenant-scoped datasets exposed by the engines.
5. Develop and maintain the per-engine service / API-client layer that consumes the REST APIs, handling the standard { success, data } response envelope, authentication / JWT tokens and fail-closed error states.
6. Ensure accessibility (GIGW / WCAG) and cross-browser, mobile-first responsiveness; optimise front-end performance (code-splitting, lazy loading, caching).
7. Collaborate with the UI/UX design, backend and QA teams to translate wireframes and requirements into functional features; write unit and component tests and participate in code reviews.

Qualifications and Experiences

1. Bachelor's degree in any discipline with 3+ years of experience in front-end web application development using React / Next.js.

Required Skill Set

1. Strong proficiency in JavaScript and TypeScript, and in React / Next.js, HTML and CSS.
2. Experience with state management (Zustand / Redux or similar), form libraries (react-hook-form) and schema validation (zod).
3. Proficiency with Tailwind CSS or equivalent, responsive / mobile-first design and component-based architecture.
4. Experience consuming REST APIs and handling authentication, tokens and error / loading states; version-control tools (Git).
5. Understanding of W3C / GIGW and accessibility (WCAG) guidelines and of Agile delivery.

Desirable Skill Set

- Experience building dynamic / metadata-driven forms and configurable UI.
- Familiarity with charting / data-visualisation libraries and dashboard development.
- Awareness of multi-tenant front-end concerns and of AI-assisted development tools.

Consolidated Remuneration:

1. Consolidated remuneration shall be commensurate with qualifications and experience within the approved project norm

General Conditions applicable to all applicants covered under this advertisement:

1. Those candidates, who are already in regular or contractual employment under Central / State Government, Public Sector Undertakings or Autonomous Bodies, are expected to apply through proper channel or attach a 'No Objection Certificate' from the employer concerned with the application OR produce No Objection Certificate at the time of interview.

2. Digital India Corporation reserves the right to fill all or some or none of the positions advertised without assigning any reason as it deems fit.

3. Candidates shall disclose any actual or potential conflict of interest with Digital India Corporation or its projects.

4. Selected candidate shall furnish an Integrity and Vigilance Declaration and shall be required to maintain highest standards of ethics.

5. Any candidate found debarred, blacklisted or convicted of offences involving moral turpitude shall not be eligible.

6. The positions are purely temporary in nature for the project of Digital India Corporation and the appointees shall not derive any right or claim for permanent appointment at Digital India Corporation or on any vacancies existing or that shall be advertised for recruitment by Digital India Corporation in future.

7. Appointment shall remain subject to verification of educational qualifications, previous employment, antecedents and character.

8. If any information furnished by the candidate is found false or suppressed at any stage, candidature/appointment shall stand cancelled without notice.

9. Selection shall be made by a duly constituted Selection Committee as approved by the Competent Authority of DIC.

10. Personal information shall be processed solely for recruitment purposes in accordance with applicable laws.

11. Digital India Corporation is an Equal Opportunity Employer.

12. The maximum age shall be as on the last date of receipt of the applications. Screening of applications will be based on qualifications, age academic record and relevant experience. The designation of the selected candidates shall be mapped as per the existing designation policy of DIC.

13. In case of a query, the following officer may be contacted

Ms. Vinaya Viswanathan

Head- HR

Digital India Corporation

Electronics Niketan Annexe,6 CGO,

Complex Lodhi Road, New Delhi – 110003

Tel.: +91 120 654 0800